

## **Trusted Computing Group's Proposed Standard For Storage Device Security**

*by Dr Robert Thibadeau and Dr Michael Willett  
Co-Chairs, Trusted Computing Group Storage Work Group*

The Trusted Computing Group (TCG) is developing an open specification for access control over features and properties of storage device computing environments. The specification extends the root-of-trust from Trusted Platform Modules on host computers to the storage devices connected to them. (A root-of-trust is a set of unconditionally-trusted functions that will work properly no matter what software is executing on the platform, providing selected security functionality.)

Storage devices such as hard disk drives, Flash memory drives, optical drives, and digital tape drives often contain processors, dynamic memory, and multiple data ports, making them vulnerable to some of the same security breaches suffered by host computers. Security solutions for storage devices already exist, such as enterprise rights management (ERM) and encryption, but each has drawbacks and vulnerabilities.

The greatest of these vulnerabilities is that personnel often do not use the solutions available to them, sometimes because they are poorly trained, or sometimes they place security low on their priority lists because they don't realize its importance. They may copy unencrypted information to take home and use on unsecured home computers or laptops, or carry that information on unprotected disks when they go on business trips.

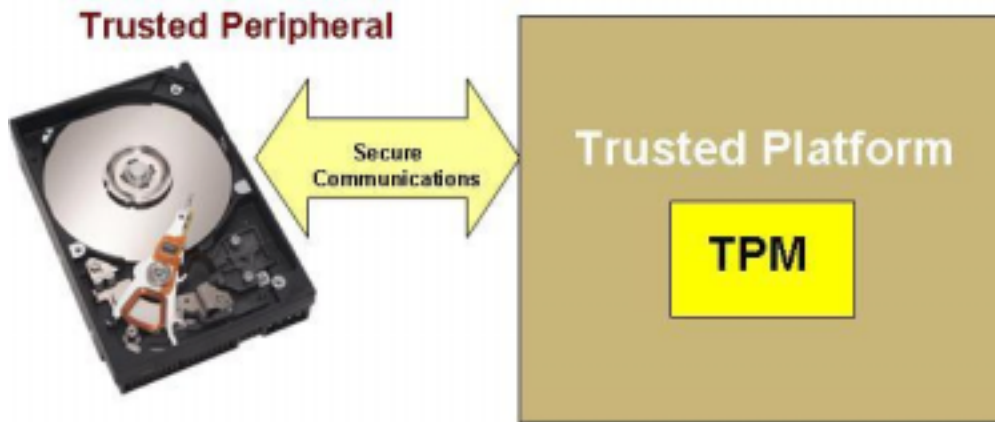
End-of-life retirement or repurposing of storage devices is an especially dangerous time, as used drives are often sold with data intact and unencrypted. Government agencies, utility companies, and universities whose personnel should have a high level of security savvy have been hit repeatedly by data breaches through loss or theft of unsecured data. A few recent examples:

- On March 11 2006 a laptop computer was stolen from a Veteran's Administration employee's home. The laptop contained unencrypted sensitive information on more than 26 million US military veterans and service members
- Also in 2006 Idaho Power sold 230 un-scrubbed disks to a salvage operator, some containing diagrams of the electric supplier's power grid, data about lawsuits stored by Idaho Power's legal department, contracts, and employee Social Security numbers, birth dates, and payroll information. The salvage operator sold 84 of them at public auction on eBay
- Used drives purchased by a security expert from the University of Cincinnati about a year ago contained criminal records; the drive was not scrubbed and the data was not encrypted

All these victims had security solutions available to them. They simply were not used.

In view of the growing number of incidents where sensitive data is lost due to human error, or negligence -- 750,000 laptops were stolen in 2005 -- security needs to be built into the storage device itself. Since storage devices are discrete computing environments unto themselves, the TCG believes they need to be protected with similar root-of-trust functions provided to host computers by Trusted Platform Modules (industry standard security chips that store digital keys, passwords and certificates securely), and they need to be complementary to and interoperate with host TPMs.

In order for the storage device to protect itself and the data entrusted to it while keeping the user experience unchanged, it is important to extend host TPM trust to the internal computing environment of all storage devices.



**Fig. 1: Storage Devices, As Well As Hosts, Need To Be Trusted**

### **Architectural Framework**

By enabling a storage device to enforce host application rights, trust is extended from the TPM-grounded host to the storage device. This allows implementations such as permanent storage areas to be restricted to particular host applications. It also gives the storage device exclusive control over its data-at-rest encryption capabilities. The storage device protects itself and the data entrusted to it but the host application, using the TPM, sets up the rules and rights.

The specification defines controllable features and properties of the storage device's internal computing environment, and provides for strong, policy driven, securely authenticated and messaged access controls over those features and properties.

### **Structure Of The Specification**

The Storage Work Group of the TCG has identified eight groups of functions performed by storage devices that need protection. The groups are described below, with a summary of how they are protected by the specification.

## Enrollment And Connection

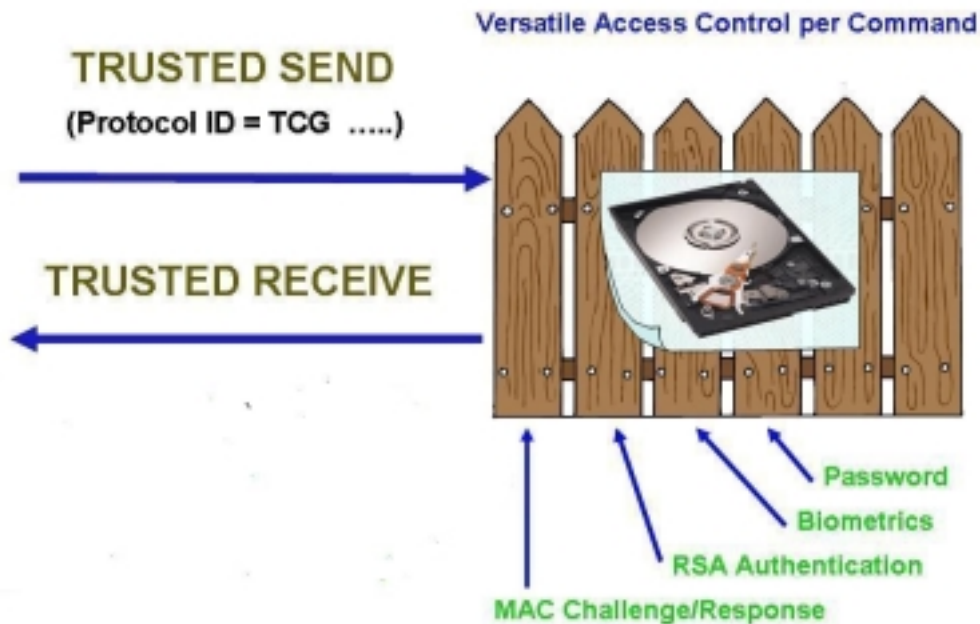
Enrollment and connection is a two-step security set-up process that provides high security while keeping the user experience as friendly as possible.

The TCG storage specification provides for both storage device-to-host and host-to-storage device mating. Storage devices can be mated to particular hosts in such a way that they will refuse to perform storage operations unless the host is authorized for access. Conversely, a host can refuse to employ a storage device in any operation unless the host can authenticate that the storage device is authorized.

The mating process takes place in two stages: enrollment and connection. Enrollment is the process by which a storage device and host are set up for connection, and begins with the authorization of the right to set up the connection. Then the authorization sequence needed by the storage device on each connection is set up.

Once the enrollment process is completed, connection between the host and storage device is automatically gated. Authorized storage devices may be freely connected and disconnected from authorized hosts without requiring passwords or other authentication credentials submitted by the user.

Since ATA and SCSI commands may be transmitted across both wired and wireless interfaces, enrollment and connection communications secrets must be confidential. Challenge-response authentication takes place in a secure session between the host and the storage device. Establishing such confidential communications extends the TPM-rooted trust in the host to the storage device.



**Fig. 2: Access Control**

## Protected Storage

Optical disks offer protected storage for many applications, such as DVD, and all storage devices that employ embedded processors have protected storage locations for system data. This protected storage is outside of the normally addressable user space and it survives intact even after the user space is repartitioned or reformatted.

Under TCG's storage specification, the process for setting up protected storage is almost identical to the two-step enrollment-connection process in mating, but in this case allows for granting a host application exclusive access to an area of protected storage. Since many different applications may need their own protected-storage spaces, the specification provides for the creation and deletion of protected storage locations separately from authorizations for their use.

## Locking And Encryption

Locking and Encryption protect addressable user space. Locking and encryption procedures process read locking and write locking separately, and can be applied to different logical partitions of the storage device. Thus the credentials needed to authorize writing or reading for one partition of user space may be different than the credentials needed to authorize writing or reading for another.

The encryption keys also may be different for one partition than for another. Encryption keys are secured by separate authorization than that needed for reading or writing authorization, although the enrollment phase for a particular partition may set, create, or fetch such keys.

## Logging

Many storage devices maintain internal logs (called SMART logs) that provide early warning of possible hard disk failure. The TCG specification provides for a simplified two-phase enrollment and use establishment for logging services to the host making use of protected storage areas.

The specification also defines a means for establishing clock time or, at minimum, a monotonic counter, so that log entries can be automatically time stamped in a protected fashion. This enables forensic logging of security violations in the host.

## Cryptographic Services

The TCG TPM is principally a pass code and public key (RSA cryptography) authentication device. In the storage industry, symmetric key and hash message authentication codes (HMAC) are also in common use. The TCG storage specification provides support for all common types of authentication algorithms for protected access to read/write operations, key management, and storage using pass code, symmetric key, HMAC, or public key authentications, which are set up in the enrollment process.

All standard cryptographic operations needed for key exchange are provided for in the specification, such as AES 128 for symmetric ciphers, SHA-1 and SHA-256 for hashing, and RSA and Elliptic Curve for public key ciphers. The modular introduction of other ciphers is also allowed for. The specification also provides for verification of signed hashes on material that must be decrypted using a key available only on the storage device.

<b>Field name</b>	<b>Description</b>
Credential serial	The unique serial number of the credential
Credential validity	The time for which the credential is valid as determined by the issuer of the credential
Credential issuer	The issuer of the credential
Credentialed	Identifies the device to which the credential applies
Device public	Holds the public key information for devices Capable of asymmetric key operations
Revocation information	Location of revocation information relevant to the credential
Supported protocols	Indicates which security protocols are supported by the device
Signature algorithm	Algorithm identifier for the signing algorithm used to sign the credential
Signature	Contains a digital signature computer computed over all fields of the credential

**Fig. 3: Components Of A Device Credential**

#### Authorizing Storage Device Feature Sets To Hosts

Enrollment sometimes requires that exclusive access to storage device feature sets be assigned to a particular host application. The TCG specification provides for the definition of a feature set that can be claimed exclusively by such an application. The exclusivity of the claim is performed by setting access controls using the storage device authentication operations.

#### Secure Download Of Firmware

The TCG specification provides that downloads of manufacturer-authorized firmware be properly authorized using strong authentication methods built into the overall architecture. In particular, downloads are hashed and the hashes signed. The storage

device confirms the signer and then publishes to the trusted platform what entities are permitted to offer downloads. Usually, this is as simple as providing a pointer to a manufacturer's certificate.

This requirement for signed downloads extends TCG trust from the TPM to the host and to the internal operations of the storage device.

### Proposed ISO ATA and SCSI commands

Since nearly all storage devices communicate through SCSI (ANSI/INCITS T10) or ATA (ANSI/INCITS T13) command sets, the specification includes proposed SCSI and ATA commands that support trusted messaging from host applications to storage device access control systems.

Because of the requirements for secure sessions, the ATA and SCSI commands proposed to T13 and T10 by the TCG serve mainly to provide a transport for TCG-defined message streams. These commands have a one-byte field for a Trusted Protocol ID. Ordinal numbers 1 - 6 are assigned to trusted protocols defined by TCG; the remainder are reserved to INCITS, or are made available for proprietary use. If the Trusted Protocol ID is set to 0, then the storage device returns a credential identifying itself. This ID can be used in enrollment and connection processes.

### **How You Can Participate**

Membership in the Trusted Computing Group is open to any corporation. The trusted storage specification is being developed by the Storage Workgroup of the Trusted Computing Group, with participation open to all TCG members of Contributor status or above. The TCG also maintains a liaison program for non-commercial organizations and individuals, and a mentor program for global outreach to scientific and educational communities.

The storage security specification, as with all TCG specifications, will be publicly available once it is completed and will be downloadable from the TCG website.

For further information on the storage security specification or membership in TCG, visit <http://www.trustedcomputinggroup.org>

### **About The Authors**

Dr Robert Thibadeau is chief technologist at Seagate Research in Pittsburgh, Pennsylvania, on long-term leave as a professor in the School of Computer Science at Carnegie Mellon University. He was one of the founding Directors of the Robotics Institute in 1980. He was one of the initiators and promoters of the concept of measurement now incorporated in the TCG's TPM. Thibadeau holds a number of patents, three of which have formed the basis for launching companies. He was the

principal contributor to the ISO/ANSI-approved SMPTE (Society of Motion Picture and Television Engineers) digital broadcast naming standards where he introduced ASN.1-based SMPTE 98e globally unique naming now in use in digital broadcasting worldwide. He is also co-chair of the Framework Committee of the International Security Trust and Privacy Alliance <http://www.istpa.org> that has introduced a basic IT framework for responsibly handling personally identifiable information. Currently Dr Thibadeau is on the Board of Directors of TCG, Chairman of the TCG Storage Workgroup, and Administrator of the TCG Mentor Program.

Dr Michael Willett, senior director at Seagate Research, received his bachelor degree from the United States Air Force Academy and masters and doctoral degrees in mathematics from North Carolina State University. After a career as a university professor of mathematics and computer science, Willett joined IBM as a design architect, later moving into the IBM Cryptography Competency Center. After retiring from IBM, Dr. Willett joined Fiderus, a security and privacy consulting practice (later bought by EDS); subsequently, he accepted a position with Wave Systems, helping to design programmable cryptographic chips and trust assurance networks. Currently Michael is on the research staff of Seagate Technology, exploring future projects in security and privacy as well as serving on several external standards bodies, including the Trusted Computing Group (TCG). Within TCG, he is Co-Chairman of the Storage Work Group.

Willett is also chair of the Privacy Framework Project of the International Security, Trust, and Privacy Alliance, developing an operational framework for converting the fair information practices into privacy services and mechanisms.

